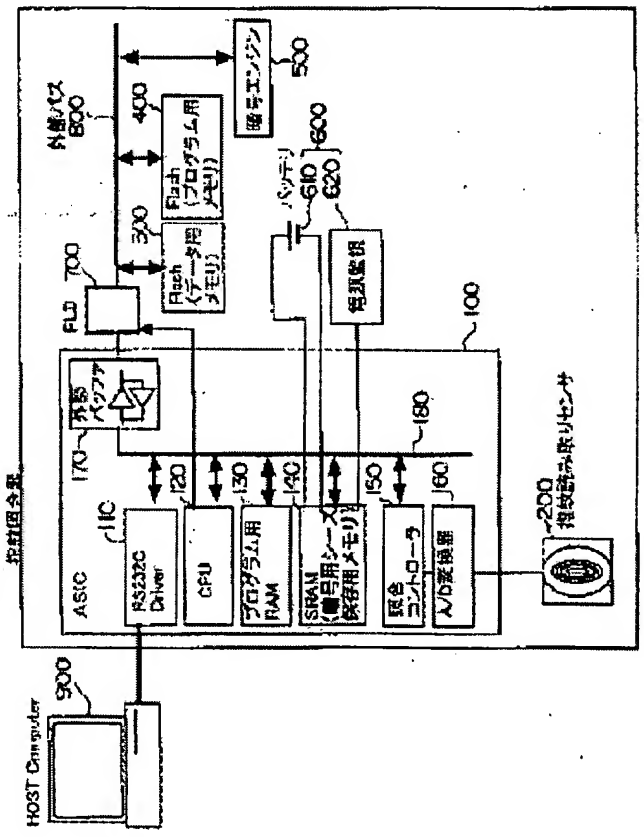
HARDWARE TOKEN WITH FINGERPRINT COLLATING FUNCTION

Publication number: JP2001357371
Publication date: 2001-12-26
Inventor: FUNABASHI TAKESHI; WADA TAKUYA
Applicant: SONY CORP
Classification:
- international: ***G06K9/00;*** **G06K9/00;** (IPC1-7): G06K19/073; H04L9/10
- european: G06K9/00A3
Application number: JP20000176549 20000613
Priority number(s): JP20000176549 20000613

Abstract of **JP2001357371**

PROBLEM TO BE SOLVED: To realize great tamper resistance technique at a comparatively low cost when an H/T using a PKI in a fingerprint collator is made merchandise. SOLUTION: When a power source is supplied, a picture is read from a fingerprint reading sensor 200 and the random number is preserved in an SRAM 140 in an ASIC 100 as a cipher key (for example, a DES key with 56 bits) for seizing a cipher. A data storing flash memory 300, a program storing flash memory 400 and a cipher engine part 500 are arranged at the outside of the ASIC 100. A fingerprint template or important data such as a PKI key are stored in the data storing flash memory 300. The cipher engine part 500 enciphers important data stored in the flash memory 300 through the use of the cipher key which is preserved in the SRAM 140 and also decodes data to be read from the flash memory 300.



F2

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－357371
（P2001－357371A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	５Ｂ０３５
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	５Ｊ１０４

審査請求　未請求　請求項の数17　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－176549(P2000－176549)

(22)出願日　平成12年６月13日(2000.6.13)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　船橋　武
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　和田　拓也
東京都品川区北品川６丁目７番35号　ソニー株式会社内

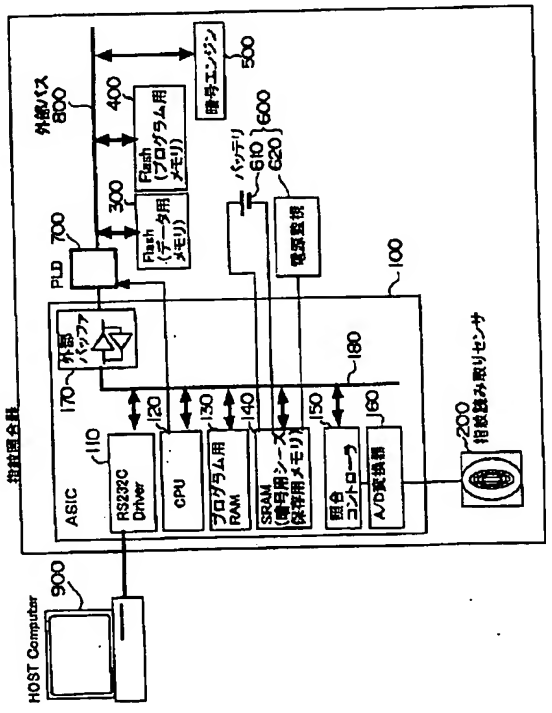
Ｆターム(参考)　5B035 AA13 BA05 BB09 BC01 CA11
CA12 CA38
5J104 AA45 JA13 KA17 NA02 NA35
NA37 NA38 NA42

(54)【発明の名称】　指紋照合機能付きハードウェアトークン

(57)【要約】

【課題】　指紋照合器にＰＫＩを使ったＨ／Ｔの商品化に際して、強力なタンパレジスタンス技術を比較的低コストで実現する。

【解決手段】　電源が投入されたとき、指紋読み取りセンサ２００から画像読み取りを行い、その乱数を暗号用シーズである暗号鍵（例えば５６ｂｉｔのＤＥＳキー）としてＡＳＩＣ１００内のＳＲＡＭ１４０に保存する。また、ＡＳＩＣ１００の外部にデータ格納用フラッシュメモリ３００と、プログラム格納用フラッシュメモリ４００と、暗号エンジン部５００を設ける。そして、データ格納用フラッシュメモリ３００には指紋テンプレートやＰＫＩ鍵等の重要データを格納する。また、暗号エンジン部５００により、ＳＲＡＭ１４０に保存した暗号鍵を用いて、フラッシュメモリ３００に記憶する重要データの暗号化を行い、またフラッシュメモリ３００から読み出すデータの復号化を行う。



【特許請求の範囲】

【請求項１】　カード型ケースの内部に指紋照合器を構成するメインＩＣを設けるとともに、前記ケースに指紋読み取りセンサを設けた指紋照合機能付きハードウェアトークンであって、
前記メインＩＣ内に設けられ、暗号用シーズを保存するための第１メモリ手段と、
前記メインＩＣの外部に設けられ、ＰＫＩ鍵及び指紋テンプレートを含む重要データを保存するための第２メモリ手段と、
前記メインＩＣの外部に設けられ、前記重要データを前記暗号用シーズによって暗号化して前記第２メモリ手段に格納するとともに、前記第２メモリ手段に格納した重要データを前記暗号用シーズによって復号化する暗号化エンジン手段と、
前記メインＩＣの外部バスを介して前記第１メモリ手段内の暗号用シーズがソフトウェアによって読み出されようとした場合に、前記第１メモリ手段の暗号用シーズを破壊する第１データ漏洩防止手段と、
前記ケースの機械的加工及び解体された場合に、前記第１メモリ手段の暗号用シーズを破壊する第２データ漏洩防止手段と、
を有することを特徴とする指紋照合機能付きハードウェアトークン。

【請求項２】　前記メインＩＣはＡＳＩＣより構成されていることを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項３】　前記第１メモリ手段は、ＳＲＡＭ、ＥＥＰＲＯＭ、フラッシュメモリ、またはプログラマブルロジックデバイスを用いることを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項４】　前記暗号化にはＤＥＳによる暗号化法を用いることを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項５】　前記暗号用シーズは、電源投入時における指紋読み取りセンサの検出信号を検出し、この検出信号によって生成した乱数をＤＥＳ鍵として用いることを特徴とする請求項４記載の指紋照合機能付きハードウェアトークン。

【請求項６】　前記乱数をバックアップのために１回だけ外部メモリ手段への記録を行うようにしたことを特徴とする請求項５記載の指紋照合機能付きハードウェアトークン。

【請求項７】　前記第１メモリ手段に記憶した乱数が前記メインＩＣの外部バスを介してモニタすることでは読み取れないように、メインＩＣと外部バスとのアイソレーションを行うバッファ手段を設けたことを特徴とする請求項５記載の指紋照合機能付きハードウェアトークン。

【請求項８】　前記第２メモリ手段に格納された重要データの読み出しは、前記指紋照合器による照合の結果、指紋の一致が判定された場合に許可することを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項９】　前記第１データ漏洩防止手段は、前記第１メモリ手段内の情報を内部ソフトウェアを書き換えて読み出そうとする行為に対して前記第１メモリ手段の暗号用シーズをソフトウェア的に破壊することを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項１０】　前記第２データ漏洩防止手段は、前記第１メモリ手段がＳＲＡＭである場合に、前記ＳＲＡＭへの通電を停止することにより、暗号用シーズをハードウェア的に破壊することを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項１１】　前記ケースを構成するカバーを固定するためのネジを前記ＳＲＡＭへの通電手段に使用することにより、前記ネジを取り外した時点で前記ＳＲＡＭへの通電が停止して暗号用シーズが破壊されるようにしたことを特徴とする請求項１０記載の指紋照合機能付きハードウェアトークン。

【請求項１２】　前記ケースに前記ＳＲＡＭへの通電を行うための配線パターンを設け、前記ケースに孔を開けた時点で前記配線パターンが破壊され、前記ＳＲＡＭへの通電が停止して暗号用シーズが破壊されるようにしたことを特徴とする請求項１０記載の指紋照合機能付きハードウェアトークン。

【請求項１３】　前記ケース内に前記ＳＲＡＭへの通電を行うための配線パターンを設けたシートを配置し、前記ケースの破損またはケースを構成するカバーの開放によって前記シートが破損し、前記ＳＲＡＭへの通電が停止して暗号用シーズが破壊されるようにしたことを特徴とする請求項１０記載の指紋照合機能付きハードウェアトークン。

【請求項１４】　前記ケースを構成するカバーの開放を検出する検出手段を有し、前記第２データ漏洩防止手段は、カバーの開放が検出された時点で前記第１メモリ手段の暗号用シーズを破壊することを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項１５】　前記外部バスのコントロールを行うプログラマブルロジックデバイスを有し、不正行為を感知した時点で、バスコントロールを破壊することにより、内部データの漏洩防止を行うことを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項１６】　前記ケース内にプリント基板上の回路素子を覆うプロテクトシートを設け、前記プロテクトシートの導体シートのショートを検出した時点で前記第１メモリ手段の暗号用シーズを破壊することを特徴とする請求項１記載の指紋照合機能付きハードウェアトークン。

【請求項１７】　前記ケース内の配線にグルーチップを挿入し、前記プロテクトシートと接着することにより、前記プロテクトシートを開放してグルーチップの導線が切断されたことを検出した時点で前記第１メモリ手段の暗号用シーズを破壊することを特徴とする請求項１６記載の指紋照合機能付きハードウェアトークン。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、各種の電子商取引等に用いられるＩＣカード等のハードウェアトークンに関し、特に不正使用防止機能を強化した指紋照合機能付きハードウェアトークンに関する。

【０００２】

【従来の技術】例えばインターネット等を使用した電子商取引は、今後一般化されることが予想され、この普及に伴って、暗証コードの盗用等による犯罪も当然のことながら増加することが予想される。これらの犯罪を未然に防ぐために、ＰＫＩ（公開鍵暗号法）による暗号鍵（秘密鍵、公開鍵）を埋め込んだＩＣカード（スマートカードともいう）等の記憶処理装置（いわゆるハードウェアトークン、以下、Ｈ／Ｔという）が実用化されようとしている。しかしながら、このようなＨ／Ｔにおいても、Ｈ／Ｔ内に設けた暗号鍵が破られると、システム全体が破壊されることになる。このため、犯罪を未然に防ぐために、各研究機関（企業等）において、色々なタンパレジスタンス（不正防止）技術を模索しているのが現状である。

【０００３】

【発明が解決しようとする課題】ところで、上述のようなＨ／Ｔにおけるタンパレジスタンスを考えた場合に、一般的には、タンパレジスタンスを強化すればするほど、Ｈ／Ｔのコストが高くなる。また、従来のＩＣカードにおいて、ＣＰＵと暗号化ＬＳＩ、及び暗号アルゴリズム用のメモリを１チップ化して、ＩＣカード内に埋め込んだ製品が提供されているが、このような１チップ化した場合、全ての処理を同一チップ内で扱うことになり、データの暗号化や復号化に時間がかかるという問題や、メモリ容量の制限から暗号鍵の拡張時の障害となるといった問題があった。さらに、暗号アルゴリズムの変更や鍵長のアップグレードの際に、設計を全面的にやり直さなければならないという問題もあった。

【０００４】そこで本発明の目的は、特に指紋照合器にＰＫＩを使ったＨ／Ｔの商品化に際して、強力なタンパレジスタンス技術を比較的低コストで実現できる指紋照合機能付きＨ／Ｔを提供することにある。

【０００５】

【課題を解決するための手段】本発明は前記目的を達成するため、カード型ケースの内部に指紋照合器を構成するメインＩＣを設けるとともに、前記ケースに指紋読み取りセンサを設けた指紋照合機能付きＨ／Ｔであって、前記メインＩＣ内に設けられ、暗号用シーズを保存するための第１メモリ手段と、前記メインＩＣの外部に設けられ、ＰＫＩ鍵及び指紋テンプレートを含む重要データを保存するための第２メモリ手段と、前記メインＩＣの外部に設けられ、前記重要データを前記暗号用シーズによって暗号化して前記第２メモリ手段に格納するとともに、前記第２メモリ手段に格納した重要データを前記暗号用シーズによって復号化する暗号化エンジン手段と、前記メインＩＣの外部バスを介して前記第１メモリ手段内の暗号用シーズがソフトウェアによって読み出されようとした場合に、前記第１メモリ手段の暗号用シーズを破壊する第１データ漏洩防止手段と、前記ケースの機械的加工及び解体された場合に、前記第１メモリ手段の暗号用シーズを破壊する第２データ漏洩防止手段とを有することを特徴とする。

【０００６】本発明の指紋照合機能付きＨ／Ｔにおいて、メインＩＣ内の第１メモリ手段には暗号用シーズが保存され、メインＩＣの外部に設けられた第２メモリ手段にはＰＫＩ鍵及び指紋テンプレートを含む重要データが保存される。また、メインＩＣの外部に設けられた暗号化エンジン手段は、上述した重要データを暗号用シーズによって暗号化して第２メモリ手段に格納し、逆に第２メモリ手段に格納した重要データを暗号用シーズによって復号化する。このように第２メモリ手段と暗号化エンジン手段をメインＩＣの外側に設けたため、暗号化等に伴うメインＩＣの負担を減らすことができ、また、暗号アルゴリズムの変更や鍵長のアップグレード等の際に、メインＩＣ側の設計変更を簡略でき、容易に設計変更を行うことができる。また、メインＩＣ内の第１メモリ手段に格納した暗号用シーズは、第１、第２データ漏洩防止手段により、ハードとソフトの両面から不正に読み取られることを防止し、強力なタンパレジスタンスを行うことができる。

【０００７】

【発明の実施の形態】以下、本発明による指紋照合機能付きＨ／Ｔ（ハードウェアトークン）の実施の形態について説明する。図１は、本発明の実施の形態による指紋照合機能付きＨ／Ｔの構成を示すブロック図である。本例の指紋照合機能付きＨ／Ｔ（指紋照合器）は、メインＩＣとしてのＡＳＩＣ１００と、指紋読み取りセンサ２００と、データ格納用フラッシュメモリ３００と、プログラム格納用フラッシュメモリ４００と、暗号エンジン部５００と、電源電池６１０及び電源監視回路６２０を有する電源バッテリ部６００と、ＰＬＤ（プログラマブルロジックデバイス）７００と、外部バス８００を有する。

【０００８】また、ＡＳＩＣ１００は、ＲＳ２３２Ｃデバイス１１０と、ＣＰＵ１２０と、プログラム用ＲＡＭ１３０と、暗号用シーズ保存用のＳＲＡＭ１４０と、照合コントローラ１５０と、Ａ／Ｄ変換器１６０と、外部

バッファ１７０と、内部バス１８０とを有する。このようなＡＳＩＣ１００において、ＲＳ２３２Ｃデバイス１１０は、ＲＳ２３２ＣによってＡＳＩＣ１００とホストコンピュータ９００とのインターフェイスをとるものである。また、ＣＰＵ１２０は、この指紋照合器全体をコントロールするものであり、プログラム用ＲＡＭ１３０は、プログラム用ワーキングＲＡＭ１３０である。

【０００９】また、ＳＲＡＭ１４０は、フラッシュメモリ３００内のデータを暗号化するための暗号用シーズを保存するメモリである。外部バッファ１７０は、ＡＳＩＣ１００内の内部バス１８０の内容がモニタできないようにするため、内部バス１８０と外部バス８００とのアイソレーションを行うものである。照合コントローラ１５０は、指紋の照合を行うエンジン部である。Ａ／Ｄ変換器１６０は、指紋読み取りセンサ２００からのアナログ画像データをデジタルデータに変換するものである。

【００１０】このＡＳＩＣ１００からは、外部バッファ１７０を介して外部バス８００が出ており、その外部バス８００に上述したデータ格納用フラッシュメモリ３００と、プログラム格納用フラッシュメモリ４００と、暗号エンジン部５００と、ＰＬＤ７００が接続されている。データ格納用フラッシュメモリ３００は、指紋用テントプレート、ＰＫＩ鍵ペア（プライベート（秘密）鍵、パブリック（公開）鍵）等の重要データが保存されている。また、プログラム格納用フラッシュメモリ４００は、各種プログラムが保存されている。また、暗号エンジン部５００は、ＰＫＩ鍵の生成と暗号化・復号化を行うものである。

【００１１】また、電源バッテリ部６００は、電源電池６１０及び電源監視回路６２０で構成されている。電源電池６１０は、ＳＲＡＭ１４０のバックアップ電源であり、指紋照合器の電源が切れても内部データの保存を行うためのものである。電源監視回路６２０は、指紋照合器の電源を監視するデバイスであり、電源が切れた状態をＡＳＩＣ１００に知らせることで、バッテリからの消費電力を小さく押さえるためのものである。また、ＰＬＤ７００は、ＡＳＩＣ１００の内部バス１８０と外部バス８００との間で信号のやりとりを制御するものである。

【００１２】以上のような構成の指紋照合器は、以下の機能を有する。

（１）指紋画像の読み取り・指紋テンプレートの保存・指紋照合機能

（２）ホストコンピュータからのデータの書き込み・読み出し・保存（保存に際しては、ＤＥＳによる暗号化を伴う）機能

（３）ＰＫＩ鍵の発生と保存・ＰＫＩ鍵による暗号化・復号化機能

（４）乱数の発生と乱数に基づくＤＥＳ鍵による暗号化・復号化機能

（５）（４）にて作成されたＤＥＳ鍵の保存機能

【００１３】次に、本例における指紋照合器の動作について順に説明する。

（２）一般的動作の説明

図２は、本例における指紋照合器の各動作を示すフローチャートであり、以下、このフローチャートを適宜用いて説明する。

（２－１）、初期動作（暗号用シーズ作成）

本例の指紋照合器に初めて電源が投入されたとき、すなわちＳＲＡＭ１４０内がオール０を検出すると（製造出荷時に０にしておく）、内部ＣＰＵ１２０は、指紋読み取りセンサ２００から、画像読み取りを行う（指が置いてない状態での読み取りのためのノイズ画像を読み取る）。このデータは、読み取り毎に常に異なる値になり（温度・湿度・電源・その他の環境差）、この値が乱数として使えることは、実験から証明済みである。そこで、この乱数値を、暗号鍵（例えば５６ｂｉｔのＤＥＳキー）としてＳＲＡＭ１４０に保存する（図２（Ａ）のステップＳ１、Ｓ２）。なお、ＳＲＡＭ１４０内のデータを暗号鍵として使う際に、外部から外部バス８００をモニタしても読むことができないように、バスアイソレーション用に外部バッファ１７０が入っている。

【００１４】（２－２）指紋の登録（ホストコンピュータ９００からの指示で行う）

指を指紋読み取りセンサ２００に置き、指紋画像を取り込む。これをＡ／Ｄ変換器１６０が２値画像に変換し、照合コントローラ１５０に送る。照合コントローラ１５０は、このデータ内の特徴部（いわゆるテンプレートという）を抽出し、ＳＲＡＭ１４０に保存されている暗号鍵（５６ｂｉｔのＤＥＳキー）で暗号化し、フラッシュメモリ３００に保存される（図２（Ｂ）のステップＳ１１、Ｓ１２）。

【００１５】（２－３）指紋の照合（ホストコンピュータ９００からの指示で行う）

指を指紋読み取りセンサ２００に置き、指紋画像を取り込む。これをＡ／Ｄ変換器１６０が２値画像に変換する。照合コントローラ１５０では、先ほど登録した、テンプレートと指紋照合を行う。この結果がＯＫ（照合一致）になると、以下のことが実行できるモードになる（なお、ホストコンピュータ９００の指示により、このモードの解除ができる）。

（Ａ）指紋の再登録

（Ｂ）ＰＫＩ暗号鍵ペアの作成

（Ｃ）ＰＫＩ暗号鍵の内、秘密鍵の使用が可能になる。

（Ｄ）データ用フラッシュメモリ３００内に記録する際にＤＥＳ鍵により暗号化する。また読み出しの際には復号化する。

【００１６】（２－４）ＰＫＩ暗号鍵ペアの作成（ホストコンピュータ９００からの指示で行う）

指紋照合がＯＫ（照合一致）になった時点で、ＰＫＩの

鍵を作成する。作成された鍵をＳＲＡＭ１４０に保存されている暗号鍵（５６ｂｉｔのＤＥＳキー）で暗号化し、フラッシュメモリ３００に記録する（図２（Ｃ）のステップＳ２１、Ｓ２２、Ｓ２３）。次に、この際、外部バス８００上に配置されている暗号エンジン部５００を使用するために、一般的に秘密鍵が外部バス８００上に現れる（外部バス８００をモニタすることで秘密鍵を盗むことが可能となる）。しかし、この行為ができるのは本人（指紋照合の結果が一致の人）のみであることから問題は生じないものである。

【００１７】（２－５）ＰＫＩ暗号鍵を使ったファイルの暗号化

次に、本例の暗号化についてファイル暗号を例に説明する。まず、ホストコンピュータ９００内で、あるファイルＦを暗号化する場合、ホストコンピュータ９００は、指紋照合器から乱数Ｒ（これをＤＥＳ鍵ｋとして使用する）を読み出す。そして、このｋを使い、ファイルＦをＤＥＳ暗号方式にて暗号化（Ｆ）^{k}する（図２（Ｄ）のステップＳ３１、Ｓ３２）。次に、このｋを、さらに指紋照合器から読み出したＰＫＩの公開鍵ｅで暗号化（ｋ）^{e}する（図２（Ｄ）のステップＳ３３）。

【００１８】（２－６）ＰＫＩ暗号鍵を使ったファイルの復号化

次に、本例の復号化についてファイル復号を例に説明する。上述のようにして暗号化されたファイル（Ｆ）^{k}を復号する場合、指紋照合がＯＫになった時点で、ホストコンピュータ９００は（ｋ）^{e}を指紋照合器に送り込む。指紋照合器内で秘密鍵ｄを使い復号し、ＤＥＳ鍵ｋを取り出してホストコンピュータ９００に送り返す（図２（Ｅ）のステップＳ４１）。このＤＥＳ鍵ｋを使い、ファイル（Ｆ）^{k}を復号しＦを復元させる（図２（Ｅ）のステップＳ４２）。

【００１９】（３）ＳＲＡＭ１４０への電力供給

（３－１）基本的な考え方。

ＳＲＡＭ１４０に保存されたＤＥＳ鍵を使い、重要なデータ（例えば、テンプレートや秘密鍵）を暗号化してから、フラッシュメモリ３００に記録する。フラッシュメモリ３００内のデータを盗むためには、ＳＲＡＭ１４０に保存されたＤＥＳ鍵を初めに取り出す必要がある。しかしながら、本例では、以下に示すような各種の漏洩防止手段によってＳＲＡＭ１４０への電源を切ることはできず（内部データが破壊する）、さらに、ソフトウェア的に取り出すことも困難にし、不正防止を行うようにしている。

【００２０】（３－２）ＳＲＡＭ１４０への電源供給

図３は、本例の指紋照合器におけるケースに設けられた電源供給用の配線構造を具体的に示す図であり、図３（Ａ）がケースを構成する上カバー１０の内面図、図３（Ｂ）がケースを構成する上カバー１０と下カバー２０とプリント基板３０を示す分解側面図、図３（Ｃ）がケースを構成する下カバー２０の上面図である。なお、プリント基板３０上には、各種回路が配置されているが、ここではＳＲＡＭ１４０と電池６１０に関して説明する。

【００２１】また、プリント基板３０は、上カバー１０と下カバー２０に挟まれており、上カバー１０と下カバー２０は、４本のネジ４０で固定されている。この固定ネジ４０が下カバー２０の孔２２Ａを通り、プリント基板３０と接触しており、かつ下カバー２０のＡ点では、プリント基板３０の配線により電池６１０の＋側につながっている。このネジ４０は、上カバー１０に設けたナット１２に螺合する。そして、上カバー１０のＡ’点のナット１２とＢ’点のナット１２とは、パターン配線１４によりカバー１０の内部で互いに接続されている。

【００２２】同様に、下カバー２０のＢ点のネジ４０は、上カバー１０のＢ’点のナット１２に接続される。また、下カバー２０のＢ点は、プリント基板３０のパターン配線３２を介してＳＲＡＭ１４０の＋側に接続されている。したがって、上カバー１０と下カバー２０がネジ４０で固定されると、パターン配線１４がＢ点のネジ４０を介してＳＲＡＭ１４０の＋側に接続される。一方、電池６１０の－側は、プリント基板３０のパターン配線３２を介してＳＲＡＭ１４０の－側に接続されていることから、ＳＲＡＭ１４０に対しての電力が供給される。図４（Ａ）は、このような配線構造を模式的に示す回路図である。

【００２３】（３－３）データ詐取

以上のような構造から本指紋照合器の稼動後に、内部データを盗もうとカバーを取り外すために、Ａ点もしくはＢ点のネジ４０を取り外した時点で、ＳＲＡＭ１４０への通電経路が破壊され、その内部に保存されているＤＥＳ鍵が破壊することになる。なお、本例では、Ａ点とＢ点の２本のネジ４０で、ＳＲＡＭ１４０への通電経路を確保しているが、もっと多くの接点を設けても良い。図４（Ｂ）は、図３（Ｃ）に示す４つの点Ａ、Ｂ、Ｃ、Ｄの各ネジ４０で通電経路を確保した場合の配線構造を模式的に示す回路図である。

【００２４】（４）ソフトウェアの書き換え

（４－１）上記の例は、メカニカルにＳＲＡＭ１４０内のデータを詐取する場合に対応する方法について説明したが、外部からファームウェアを書き換えることでＳＲＡＭ１４０内データを詐取することも考えられる。しかしながら、本例では、ホストコンピュータ９００からファームウェアを書き換えるためのコマンドが発行された時点で、ＳＲＡＭ１４０内のデータ（ＤＥＳ鍵）がソフト的に破壊されるようになっている。これにより、外部からのファームウェアの書き換えによるデータ詐取を阻止することができる。

【００２５】（５）初期動作においてＳＲＡＭ１４０内へのＤＥＳ鍵保存

（５－１）上述のような仕組みにより、ＳＲＡＭ１４０内のデータ、及びフラッシュメモリ３００内の重要データの詐取をきわめて難しくすることができるが、逆に、電池６１０切れや、修理等によりカバーを外す場合に、本人でさえ重要データの読み出しができなくなる問題が出てくる。そこで、（２－１）においてＳＲＡＭ１４０に乱数を保存した直後に、１回だけ、例えばフロッピディスク等の外部メモリ手段に同じデータをバックアップとして保存する。このバックアップ処理は、ソフトウェアでコントロールする。また、バックアップをとったことを示す印（フラグ等）をＳＲＡＭ１４０上に記録する。そして、この印がある場合は、２度とバックアップはとれないようにする。

【００２６】（５－２）電池６１０が切れた場合の交換時の対応として、図４（Ａ）に示すように、電池６１０とパラレルにコンデンサ６３０を配置しておく。電池交換時の短時間は、このコンデンサからＳＲＡＭ１４０への電源供給を行う。

【００２７】以上にように、本例によれば、ＡＳＩＣ１００内に非常に少ない容量（５６ビットのＤＥＳキーである場合、８バイトで良い）のＳＲＡＭ１４０を配置し、暗号エンジン部５００をＡＳＩＣ１００の外部に配置することにより、ＡＳＩＣ１００の変更を行うことなく、比較的容易に暗号アルゴリズムの変更や、鍵長変更が可能になる。さらに、データ保存用フラッシュメモリ（秘密鍵や指紋テンプレート保存用）３００をＡＳＩＣ１００の外部に配置することにより、ＡＳＩＣ１００に影響を及ぼすことなく、重要データの大きさに制限が無くなり、自在に機能拡張等を行うことが可能となる。さらに指紋照合器とＰＫＩを組み合わせたハードウェアトークンという商品化において、各種のデータ漏洩防止手段により、強力なタンパレジスタンス機能を提供することが可能となる。

【００２８】次に、本実施の形態における応用例について説明する。

（６）応用例１

（６－１）カバーを外さずに孔開け等の不正な加工を行う方法への対応（図５）

上述のようなケースの構造においてカバー１０、２０を外さずに孔を開けることにより、プリント基板３０上の外部バスをモニタすることで、ＳＲＡＭ１４０内のデータを盗み出す方法が考えられる。そこで、図５（Ａ）に示すように各カバー１０、２０の内面に１本の線を蛇行させて形成したパターン配線（本例ではメッシュ配線という）１６、２６によって、カバー１０、２０に孔を開けた時点で、ＳＲＡＭ１４０への電源供給を切る方法である。上述した例と同様にプリント基板３０は、上カバー１０と下カバー２０に挟まれており、上カバー１０と下カバー２０は、４本のネジ４０で固定されている。固定ネジ４０が、下カバー２０の孔２２Ａを通り、プリント基板３０と接触しており、かつ下カバー２０のＡ点では、プリント基板３０のパターン配線３２により電池６１０の＋側につながっている。

【００２９】このネジ４０は、上カバー１０に設けたナット１２に螺合する。そして、上カバー１０のＡ’点から上カバー１０内の配線１６により、Ｄ’点に接続されている。下カバー２０のＤ点のネジ４０が、Ａ点同様に固定されるとプリント基板３０の配線３２により、Ｄ点とＣ点が接続される。そして、Ｃ点のネジ４０を介してプリント基板３０に接続され、このＣ点からプリント基板３０の配線３２により、ＳＲＡＭ１４０の＋側に接続される。ＳＲＡＭ１４０の－側は、プリント基板３０の配線３２により、電池６１０の－側に接続されている。さらに電源供給ラインとして、Ａ点がプリント基板３０の配線により電池６１０のプラスにつながっている。これにより、ＳＲＡＭ１４０に対しての電力が供給される。

【００３０】（６－２）プリント基板３０上の電池６１０、ＡＳＩＣ１００、及び外部バス８００の露出部にメッシュシートを付加する方法（図６）

このメッシュシート５０は、４本のネジ４２でプリント基板３０上に取り付けられる。プリント基板３０上のＡ点からメッシュシート５０上のパターン配線５２によりＤ点に接続され、Ｄ点からＣ点はプリント配線により接続され、Ｃ点からＢ点はメッシュシート５０上の配線５４により接続されている。そして、ＳＲＡＭ１４０の－側は電池６１０の－側にプリント配線により接続され、Ｂ点からＳＲＡＭ１４０の＋側に接続されている。したがって、メッシュシート５０がネジ４２で固定されると、ＳＲＡＭ１４０への電源供給が行われる。そして、メッシュシート５０を外すか、孔を開けた時点でＳＲＡＭ１４０への電源供給が切れることになる。

【００３１】（６－３）電池６１０の代わりにコンデンサを使う

上述した例では、ボタン電池６１０を想定しているが、これに限らずリチャージャブルな電池やコンデンサによってバックアップすることも可能である。

【００３２】（７）応用例２

（７－１）ＥＥＰＲＯＭによるタンパレジスタンス技術

上述した例では、ＳＲＡＭ１４０を使用する例を説明したが、ＡＳＩＣ１００内にＳＲＡＭ１４０の代わりにＥＥＰＲＯＭやフラッシュメモリを使うことも考えられる。この場合、電池６１０は必要なくなり、上述のような通電停止によるデータの破壊を行うことはできないが、この場合には例えば次の応用例２を採用することができる。

【００３３】（７－２）上述した（６）の方法（通電停止）と全く逆の方法で積極的に破壊（図７）

上述した応用例１では、電池６１０からの電源を常に入れておくことを利用してデータの漏洩防止を図ったが、

逆にカバー（ケース）を開けた時に、内蔵電池６１０がONになり、それをセンスしたＣＰＵ１２０がＳＲＡＭ１４０の代わりに設けたフラッシュメモリやＥＥＰＲＯＭ内のデータ（ＳＲＡＭ１４０の場合と同様にＤＥＳ鍵が保存されている）を破壊する方法も考えられる。これは、図７に示すように、上カバー１０を開けると、リリースピン６０が持ち上がり、電池（ボタン電池）６１０に板ばねよりなるばね接点６２が接触する。これにより、例えホストコンピュータ９００からの電源が切れていても、指紋照合器への電源が入り、かつそれをセンスしたＣＰＵ１２０がフラッシュメモリ、ＥＥＰＲＯＭ内のデータ（乱数によるＤＥＳ鍵）を破壊する。この場合のメリットは、常時通電が必要なＳＲＡＭを使わないことにより、電池６１０の消耗を大幅に改善できるとともに、適正な電池交換操作ではデータを破壊しないため、電池交換時を含めて誤って通電を停止してしまい、データを破壊してしまうことも極めて少なくなる。

【００３４】（７－３）ＰＬＤの破壊（図８）

上述したＰＬＤ７００内に前もって、外部バス８００のコントローラを内蔵しておく。そして、カバーが外された時点で、ＣＰＵ１２０によってコントローラを破壊する。それ以後、全体的に動作不能になる。さらに、図８に示すように、ＰＬＤ７００内のメモリ７１０に上述した乱数（ＤＥＳ鍵）、あるいは、ＤＥＳの暗号アルゴリズムも入れておく。これにより、カバーが取り外された際に、ＰＬＤ７００内のデータを破壊することも考えられる。

【００３５】（８）応用例３

（８－１）上述した図３～図６に示したデータ漏洩防止手段では、ケースを構成するカバーを取り外したり、孔を開けることにより、ＳＲＡＭ１４０への通電経路が壊れ、内部のデータを破壊するようにしたが、この場合、通電経路を構成するネジ４０の間をケースの外側で導線によって接続した後、カバーの一部を破壊したり、カバーに孔を開けたりすることにより、内部のプリント基板３０上の外部バスをモニタすることで、ＳＲＡＭ１４０内のデータを盗み出す方法が考えられる。もちろん、上述した図３～図６の方法では、タンパエビデンス（不正に破壊した証拠を残す）としては有効があるが、完全なタンパレジスタンス（不正防止）としては、さらに改良の余地のあるものである。

【００３６】また、上述した例では、フラッシュメモリへのプログラムロード時には、ソフト的に内部データを破壊することで、偽物のソフトウェアロードによる乱数読み出し犯罪を防いでいる。しかし、この場合、上述した上カバーやメッシュシートを取り去った後に、プリント基板上のフラッシュメモリを偽物のプログラムが記憶されているフラッシュメモリに物理的に交換し、ＳＲＡＭ内の乱数を読み出すことが可能となる。そこで、以下の応用例３では、このようなケースの外部に導線を設けるような巧妙な不正行為に対しても、データ漏洩を防止する手段について説明する。

【００３７】（８－２）プロテクトシート構造（図９）

プロテクトシート７０は、２枚の導体シート（全面に導体膜が行き渡ったシート形状のもので配線ではない）７２Ａ、７２Ｂを、数ミクロン（例えば２μｍ）という非常に薄く、かつ、柔らかい絶縁フィルム７４で電気的に分離した構造を有する。また、さらに各導体シート７２Ａ、７２Ｂの外側全面を保護シート７６Ａ、７６Ｂによって挟んだ構造となっている。そして、このようなプロテクトシート７０を切断、あるいは孔開けした場合には、絶縁フィルム７４による絶縁状態が壊れ、導体シート７２Ａ、７２Ｂが電気的に導通することになる。したがって、このようなプロテクトシート７０をカバー１０、２０の内側等に配置し、各導体シート７２Ａ、７２Ｂの導通状態をＡＳＩＣ１００で監視することにより、カバー１０、２０の不正な加工を検出し、内部データの破壊を行うようにする。

【００３８】（８－３）グルーチップ構造（図１０）

グルーチップ８０は、適当な大きさを有するプラスチックモールド部品８２Ａ、８２Ｂで、１本の導線（銅線）８４を埋め込んだものである。この導線８４の両端がプラスチックモールド部品８２Ａ、８２Ｂから外側に延出ており、プリント基板上で配線の一部を担うものである。したがって、このようなグルーチップ８０をプリント基板３０の配線に挿入することにより、ケースに不正な加工が加えられた場合の導線８４の分断を検出でき、内部データの破壊を行うようにする。

【００３９】（８－４）全体構造の具体例（図１１）

製造組み立ての方法として、図１１に示すように、ＡＳＩＣ１００とフラッシュメモリ３００／４００の中間と外側に合計３つのグルーチップ８０が配置されている。そして、グルーチップ８０の上部にエポキシ樹脂系等の接着剤９０が塗布され、その上面にプロテクトシート７０が配置される。プロテクトシート７０は、４つのコーナ部Ａ、Ｂ、Ｃ、Ｄをプリント基板３０の上面にネジ止めまたは半田付け等によって取り付けられている。

【００４０】（８－５）回路の構成

プロテクトシート７０及びグルーチップ８０は、それぞれプリント基板３０の配線に接続されている。まず、プリント基板３０上で、電池の＋電極は図１１のＡ点に配線されており、Ａ点からプロテクトシート７０の＋側導体シート７２Ｂにネジまたは半田により接続されている。さらに、＋側導体シート７２ＢはＣ点に接続されている。そして、このＣ点からネジを介してプリント基板３０上の配線に接続され、その後、３つのグルーチップ８０を介してＳＲＡＭ１４０の＋側に配線されている。次に、電池の－電極がＢ点に配線されており、Ｂ点からプロテクトシート７０の－側導体シート７２Ａにネジまたは半田によって接続されている。さらに、この－側導

体シート７２Ａは、Ｄ点に接続されており、このＤ点からプリント基板３０の配線を介してＳＲＡＭ１４０の一側に接続されている。

【００４１】（８－６）犯罪行為

以上のような構成において、例えば上述したＡ点とＣ点を導体で接続し、さらにＢ点とＤ点を接続し、その後、プロテクトシート７０をはがそうとすると、グルーチップ８０がプロテクトシート７０側に接着剤９０で接着されているため、外れてしまい、電気回路的に切断されることになる。したがって、これをＡＳＩＣ１００側で検出し、ＳＲＡＭ１４０内のデータを破壊する。また、プロテクトシート７０に孔を開けたり、切断した場合には、＋側と－側がショートし、やはりＳＲＡＭ１４０内のデータを破壊する。なお、データ漏洩防止手段の具体的な構成としては、上述した例に限らず、例えばカバーの開放を検出する手段として各種のセンサ等が考えられることから、これらセンサ等と上述した各種の方法を汲み合わせるように構成し得ることはもちろんである。

【００４２】

【発明の効果】以上説明したように本発明の指紋照合機能付きＨ／Ｔは、メインＩＣ内に設けられ、暗号用シーズを保存するための第１メモリ手段と、メインＩＣの外部に設けられ、ＰＫＩ鍵及び指紋テンプレートを含む重要データを保存するための第２メモリ手段と、メインＩＣの外部に設けられ、重要データを暗号用シーズによって暗号化して第２メモリ手段に格納するとともに、第２メモリ手段に格納した重要データを暗号用シーズによって復号化する暗号化エンジン手段と、メインＩＣの外部バスを介して第１メモリ手段内の暗号用シーズがソフトウェアによって読み出されようとした場合に、第１メモリ手段の暗号用シーズを破壊する第１データ漏洩防止手段と、ケースの機械的加工及び解体された場合に、第１メモリ手段の暗号用シーズを破壊する第２データ漏洩防止手段とを有することを特徴とする。

【００４３】このため、本発明の指紋照合機能付きＨ／Ｔでは、第２メモリ手段と暗号化エンジン手段をメインＩＣの外側に設けたため、暗号化等に伴うメインＩＣの負担を減らすことができ、また、暗号アルゴリズムの変更や鍵長のアップグレード等の際に、メインＩＣ側の設計変更を簡略でき、容易に設計変更を行うことができる。また、メインＩＣ内の第１メモリ手段に格納した暗号用シーズは、第１、第２データ漏洩防止手段により、ハードとソフトの両面から不正に読み取られることを防止し、強力なタンパレジスタンスを行うことができる。したがって、指紋照合器にＰＫＩを使ったＨ／Ｔの商品化に際して、強力なタンパレジスタンス技術を比較的低コストで実現できる指紋照合機能付きＨ／Ｔを提供することができる効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態による指紋照合機能付きＨ／Ｔの構成例を示すブロック図である。

【図２】図１に示す指紋照合機能付きＨ／Ｔの各動作を示すフローチャートである。

【図３】図１に示す指紋照合機能付きＨ／Ｔの配線パターンの一例を示す図であり、図３（Ａ）は上カバーの内面図、図３（Ｂ）は上下カバーとプリント基板の分解側面図、図３（Ｃ）は下カバーの内面図である。

【図４】図４（Ａ）は図３に示す配線パターンの模式的に示す回路図、図４（Ｂ）は図４（Ａ）の変形例を示す回路図である。

【図５】図１に示す指紋照合機能付きＨ／Ｔの配線パターンの他の例を示す図であり、図５（Ａ）は上カバーの内面図、図５（Ｂ）は上下カバーとプリント基板の分解側面図、図５（Ｃ）は下カバーの内面図である。

【図６】図１に示す指紋照合機能付きＨ／Ｔの配線パターンのさらに他の例を示す平面図である。

【図７】図１に示す指紋照合機能付きＨ／Ｔのケースの開放を検出する構成を示す図であり、図７（Ａ）は上下カバーとプリント基板の分解側面図、図７（Ｂ）は回路図である。

【図８】図１に示す指紋照合機能付きＨ／Ｔに設けたＰＬＤの構成例を示すブロック図である。

【図９】図１に示す指紋照合機能付きＨ／Ｔに設けるプロテクトシートの一例を示す図であり、図９（Ａ）は平面図、図９（Ｂ）は側断面図である。

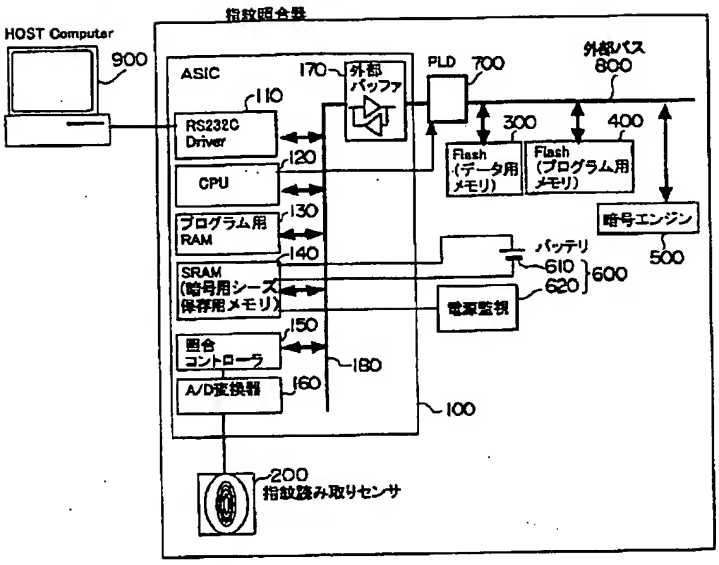
【図１０】図１に示す指紋照合機能付きＨ／Ｔに設けるグルーチップの一例を示す側面図である。

【図１１】図９に示すプロテクトシートと図１０に示すグルーチップを指紋照合機能付きＨ／Ｔのプリント基板上に設けた例を示す平面図である。

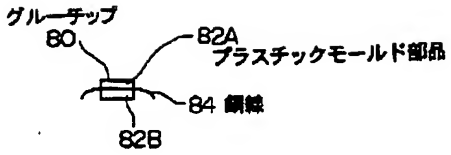
【符号の説明】

１０…上カバー、２０……下カバー、３０……プリント基板、４０……ネジ、１００……ＡＳＩＣ、１１０……ＲＳ２３２Ｃデバイス、１２０……ＣＰＵ、１３０……プログラム用ＲＡＭ、１４０……暗号用シーズ保存用ＳＲＡＭ、１５０……照合コントローラ、１６０……Ａ／Ｄ変換器、１７０……外部バッファ、１８０……内部バス、２００……指紋読み取りセンサ、３００……データ格納用フラッシュメモリ、４００……プログラム格納用フラッシュメモリ、５００……暗号エンジン部、６００……電源バッテリ部、６１０……電源電池、６２０……電源監視回路、７００……ＰＬＤ、８００……外部バス、９００……ホストコンピュータ。

【図１】

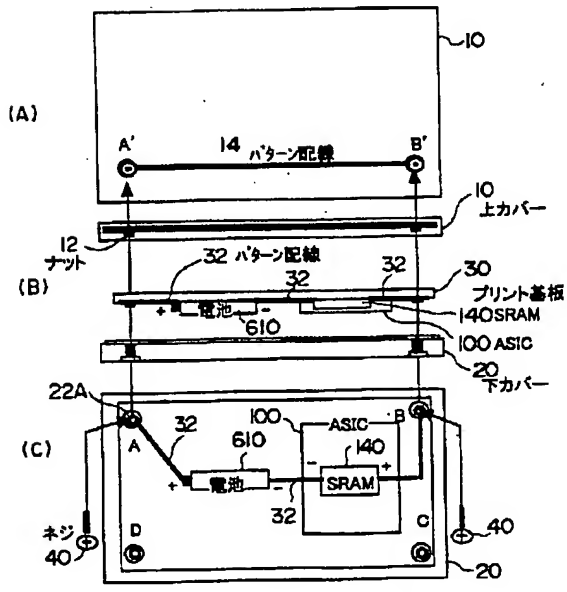


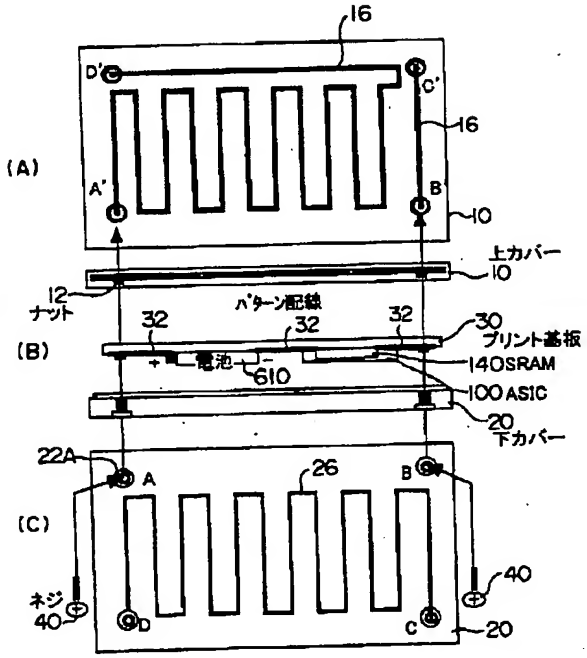
【図１０】



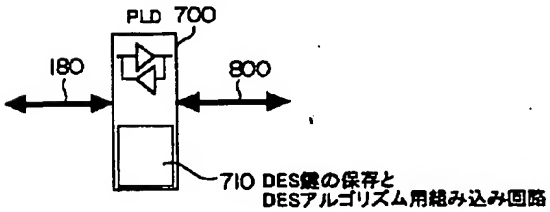
【図３】

【図５】

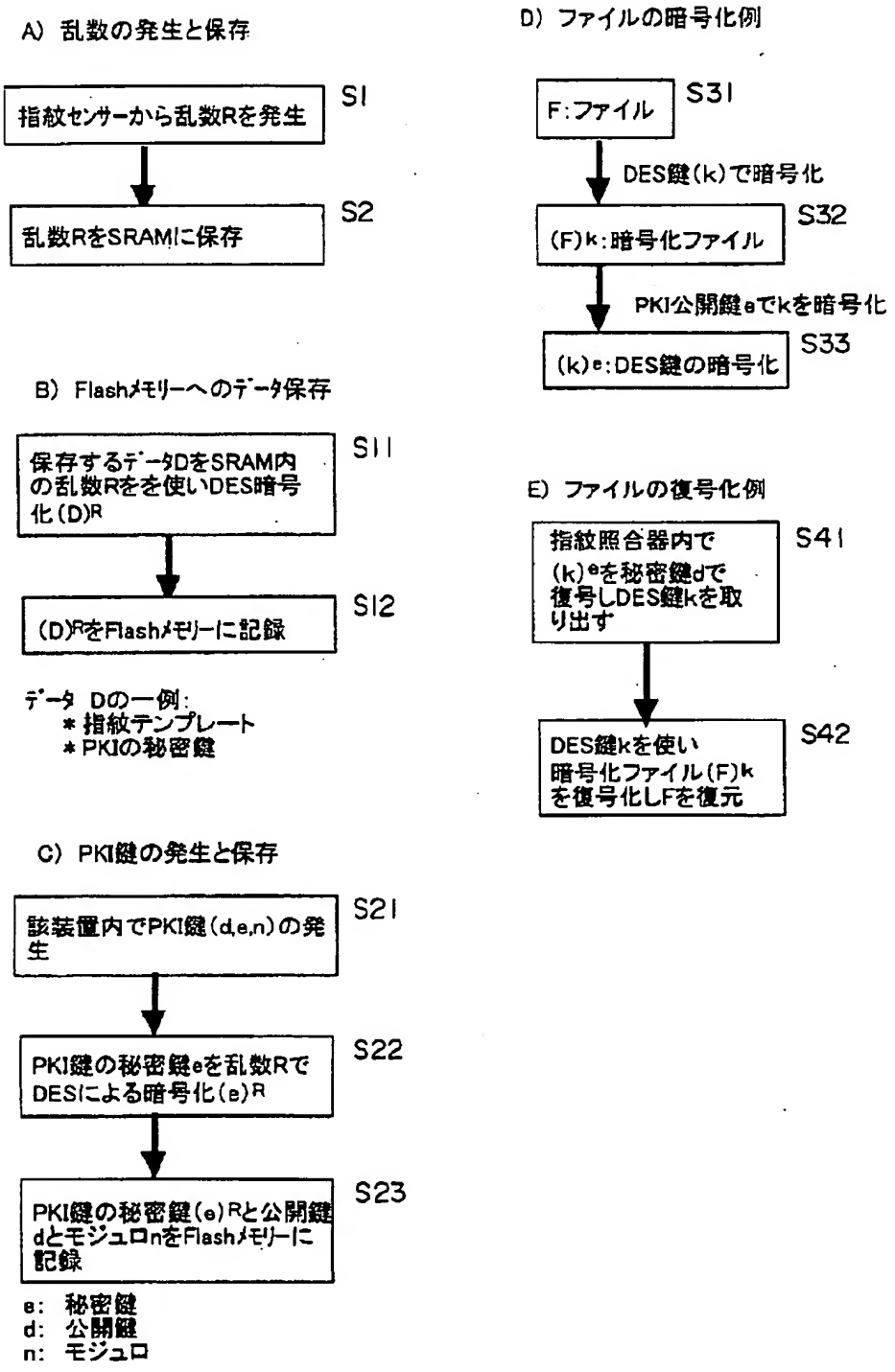




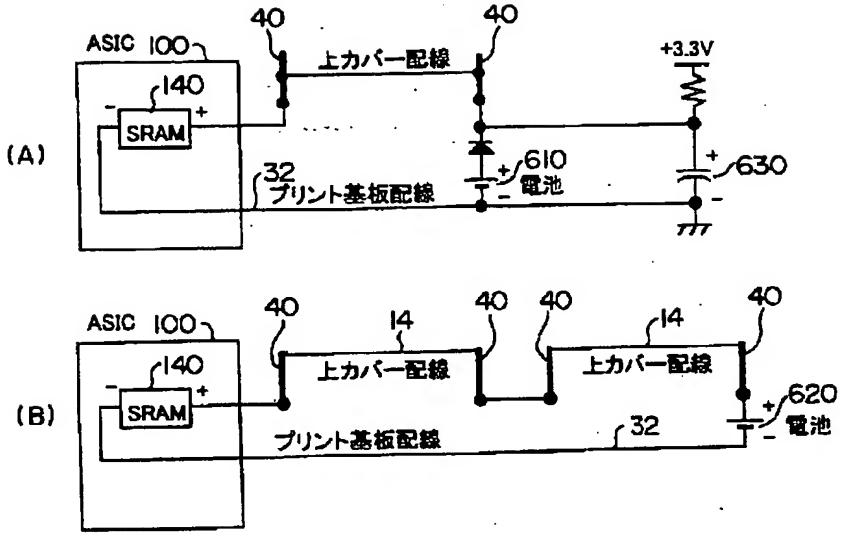
【図８】



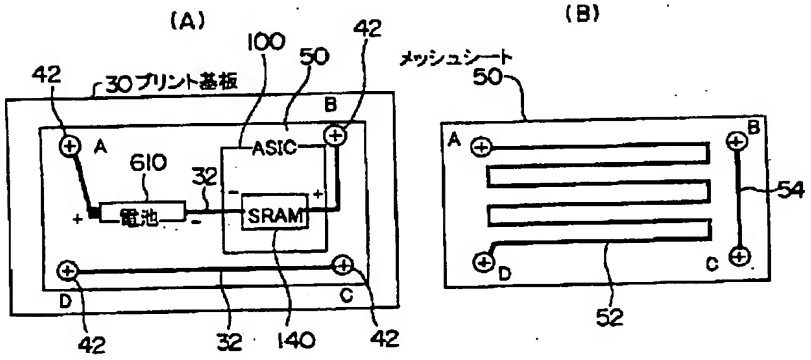
【図２】


A) 乱数の発生と保存
指紋センサーから乱数Rを発生
S1
乱数RをSRAMに保存
S2
B) Flashメモリーへのデータ保存
保存するデータDをSRAM内の乱数Rをを使いDES暗号化(D)R
S11
(D)RをFlashメモリーに記録
S12
データ Dの一例:
* 指紋テンプレート
* PKIの秘密鍵
C) PKI鍵の発生と保存
該装置内でPKI鍵(d,e,n)の発生
S21
PKI鍵の秘密鍵eを乱数Rで DESによる暗号化(e)R
S22
PKI鍵の秘密鍵(e)Rと公開鍵dとモジュロnをFlashメモリーに記録
S23
e: 秘密鍵
d: 公開鍵
n: モジュロ
D) ファイルの暗号化例
F:ファイル
S31
DES鍵(k)で暗号化
(F)k:暗号化ファイル
S32
PKI公開鍵eでkを暗号化
(k)e:DES鍵の暗号化
S33
E) ファイルの復号化例
指紋照合器内で (k)eを秘密鍵dで復号しDES鍵kを取り出す
S41
DES鍵kを使い 暗号化ファイル(F)k を復号化しFを復元
S42

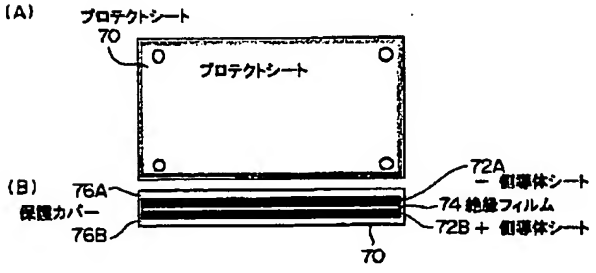
【図４】


(A)
ASIC 100
140
SRAM
40
上カバー配線
40
+3.3V
610
電池
630
32
プリント基板配線
(B)
ASIC 100
140
SRAM
40
14
40
40
14
40
620
電池
32
プリント基板配線

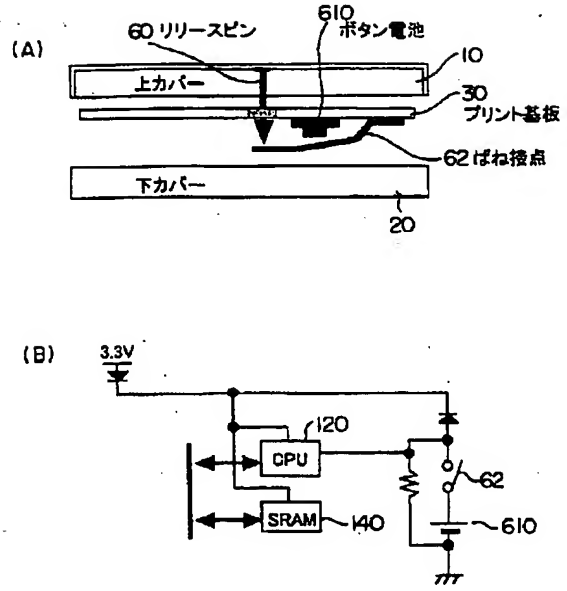
【図６】


(A)
(B)
100
50
42
42
30プリント基板
メッシュシート
50
A
B
610
32
ASIC
SRAM
電池
54
D
C
52
42
32
140
42

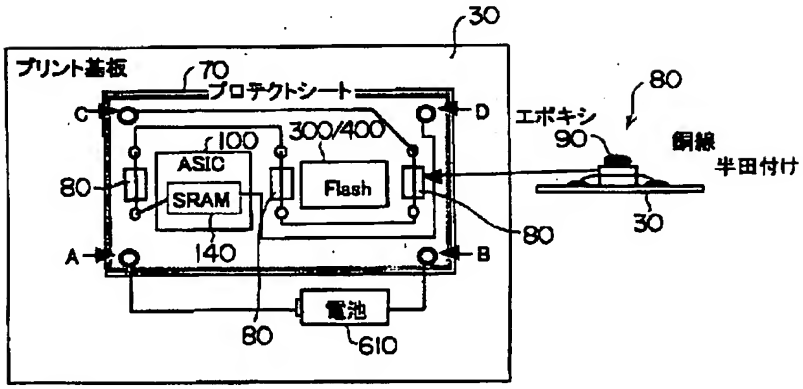
【図９】


(A)
プロテクトシート
70
プロテクトシート
(B)
76A
保護カバー
76B
72A
－ 側導体シート
74 絶縁フィルム
72B ＋ 側導体シート
70

【図７】


(A)
60 リリースピン
610
ボタン電池
10
上カバー
30
プリント基板
62 ばね接点
下カバー
20
(B)
3.3V
120
CPU
62
SRAM
140
610

【図１１】


30
プリント基板
70
プロテクトシート
C
D
100
300/400
ASIC
SRAM
Flash
80
140
A
B
80
80
電池
610
エポキシ
90
銅線
半田付け
30